Survivability Analogy for Cloud Computing

Siyakha N. Mthunzi
Cloud Computing and Applications Research Lab
School of Computing, and Digital Technologies .
Staffordshire University, College Road, ST4 2DE - Stoke-on-Trent, UK
Siyakha.mthunzi@staffs.ac.uk

Elhadj Benkhelifa
Cloud Computing and Applications Research Lab
School of Computing, and Digital Technologies.
Staffordshire University
College Road, ST4 2DE - Stoke-on-Trent, UK
E.Benkhelifa@staffs.ac.uk

***Abstract*—As cloud computing has become the most popular computing platform, and cloud-based applications a commonplace, the methods and mechanisms used to ensure their survivability is increasingly becoming paramount. One of the prevalent trends in recent times is a turn to nature for inspiration in developing and supporting highly survivable environments. This paper aims to address the problems of survivability in cloud environments through inspiration from nature. In particular, the community metaphor in nature's predator-prey systems where autonomous individuals' local decisions focus on ensuring the global survival of the community. Thus, we develop analogies for survivability in cloud computing based on a range of mechanisms which we view as key determinants of prey's survival against predation. For this purpose we investigate some predator-prey systems that will form the basis for our analogical designs. Furthermore, due to a lack of a standardized definition of survivability, we propose a unified definition for survivability, which emphasizes as imperative, a high level of proactiveness to thwart black swan events, as well as high capacity to respond to insecurity in a timely and appropriate manner, inspired by prey's avoidance and anti-predation approaches.**

Keywords—Survivability; Predator-prey; Cloud-computing; Analogie

I. INTRODUCTION

In the military context, survivability contemplates damage tolerance and avoidance, i.e. vulnerability, recoverability, and susceptibility, as central and congruent to survivability assessment and decision-making. In nature, several biological theories describe survivability through evolutionary principles and concepts such as adaptation. In the computing domain, survivability research is said to have advanced due to the development of critical infrastructures such as telecommunications networks, power grids, etc. In this context, the notion of survivability is deeply aligned with the accidental attacks. Four survivability themes can thus be identified; resistance (ability to repel an attack), intrusion detection (ability to recognize an intrusion), recovery (capacity to resume complete and/or essential services after fault, failure or attack), and adaptation (capacity to evolve to cope with similar attacks, faults or failures).

In cloud computing environments, survivability revolves around the wide adoption of virtualisation technologies, broad network access and on-demand nature of services and resources. More critical to survivability in the cloud-computing context, is the complexity of the security landscape, which is an underlying issue central to this paper. Traditional computing environments' concerns revolved around security, i.e. confidentiality, integrity, and availability of information. In contrast, cloud computing's concerns are multi-faceted. In addition to its service aspect, its outsourcing element, its un-perimeterised nature, and accessibility over the internet, security in cloud computing should be viewed in unison with survivability. In fact, one would argue that cloud computing research requires greater focus and attention towards standardizing survivability, including its definition and developing a standard survivability concept. Nonetheless, survivability is viewed as a product of an appropriate combinations of variables (closest combination with correct magnitudes, parameters, etc.), such that its magnitude depends on the role of individual variables and the stages in life history of each entity [1]. According to the authors, the following are factors upon which survivability can be evaluated: resistance to deleterious agents, competitive saprophytic ability, responsiveness, and multinational capability. Here, resistance to deleterious agents encompasses environmental dynamics such as temperature and radiation upon which survival may be attributed. Similarly, competitive saprophytic ability highlights active actions or processes in which fungi that rapidly grows and germinate to develop good enzymes which develop impeccable capacity to produce antibiotics, but tolerance the same antibiotics from other sources, acting as a sure way for survival [1]. Furthermore, mutational capacity which is responsible for protein synthesis is viewed as a predicate for adaptation and survivability of body cells. Thus, bility according to how li within their environment. It is reasonable based on the foregoing, to imagine survivability as the reliance upon the timely recognition of changes in the environment, to implement necessary responses.

Due to the lack of standardized definition of survivability, [2] recommends the following as basic components for survivability: a definition which distinguishes the

environments for which it is defined, an identified and clarified type of threat to survivability should be identified, for instance, attacks that are intentional or accidental, or faults and errors, the ability to adapt in the event of a threat to ensure a continued provision of services, acceptable level of service continuity, and timeous service provision.

This paper aims to address survivability in cloud computing environments, i.e. the ability to continue providing services under deliberate attack, using an analogous system in nature. An analogical approach is suitable not only because it is a systematic method to transfer concepts across domains, but aids in developing a comprehensive definition of survivability for cloud computing environments, principally inspired by nature's well-tested systems. In addition, the analogical approach offers the following benefits:

- Represents common behaviors, mechanisms and methods.
- Developed as modular components enabling system modelling to scale with new additional features.
- Simplicity of analogies enables the deconstruction of otherwise complex behaviours.
- Enables the extraction of secondary survival mechanisms, for instance, where prey parents resort to mobbing, counter-attack or sacrificing off-springs to increase survival chances for the majority. This analogy can therefore be reused regardless of its initial outcome.

II. BACKGROUND

Apart from semantics around the definition of survivability, there seems to be a consensus on the core areas closely related to survivability. Such areas include resilience, dependability, fault-tolerance, assurance, fault-tolerance, availability, performability, etc. Since survivability in this research focuses upon the security context of cloud infrastructures, survivability reviews considered in this section will focus upon the functionality of components of computing infrastructures individually, as well as a networked system in its entirety. [3] coined the term survivability-over-security (SOS) to describe the survivability goals of simultaneously reducing sum vulnerabilities which increasing recovery and flexibility in networked systems. These authors however digress from the view postulated in this research, that the survivability of individual system components is indeed vital to the overall survivability of an entire networked system. A case in point in cloud environments is cloud computing storage security, which encompasses storage components such storage isolation, data recovery, storage place as determinants of long-term data survivability [4]. Table 1 below is a summary of some prominent definitions from [2]'s survey of survivability?

In the predator-prey dynamic, predation is said to increase the probability of prey extinction, itself an indicator of the survivability of that specie [5]. Prey populations survivability is impacted by an interaction of demographic, environmental and genetic factors [6]. Discovering the critical survival mechanisms for cloud environments considers both, the subjective and objective selection of anti-predator and predation avoidance mechanisms (techniques and behaviours) employed prey species. Mechanisms may exist as specific (where mechanisms are effective against a specific predator), or non-specific (where strategies are effective against all predators) [7]

TABLE 1. SUMMARY OF AVAILABLE DEFINITIONS FOR SURVIVABILITY

NO	DEFINITION
1	To provide quantitative measures for the network's capability to tolerate failures and to provide continuous service.
2	Defined in terms of network survivability where it is (1) the ability of a network to maintain or restore an acceptable level of performance during network failure conditions by applying various restoration techniques and (2) the mitigation or prevention of service outages from potential network failures by applying preventative techniques.
3	The quality of a system to handle all essentially critical operation instances successfully.
4	The capability of a system to fulfil its mission in a timely manner in the presence of attacks, failures, or accidents.
5	The ability of a system to continue operation despite the presence of abnormal events such as failures and intrusions.
6	A network's ability to perform its designated set of functions given network infrastructure component failures, resulting in a service outage, which can be described by the number of services affected, the number of subscribers affected, and the duration of the outage.
7	Robustness under conditions of intrusion, failure, or accident.
8	The ability of a system to maintain a set of essential services despite the presence of abnormal events such as faults and intrusions.
9	That a system can be made robust to partially successful attack through general architecture features, through adaptability (flexible response to unanticipated changes) and flexibility (ability to adapt to a range of adverse events without having to anticipate the response in advance).
10	To provide network design and management procedures towards minimizing the impact of failures on multi-networks.
11	The ability of a system to tolerate intentional attacks or accidental failures or errors.
12	Defined in terms of information survivability where it is the ability of an information system to continue to operate in the presence of faults, anomalous system behaviour, or malicious attack.
13	The ability of a system to provide service (possibly degraded) when various changes occur in the system or operating environment.
14	Where network systems continue functioning even when under attack.
15	The ability of a system/network to be maintained in the working state, given that a deterministic set of failures occurs to the system/network; therefore, the survivability is always "yes" or "no" for a given failure scenario.
16	Phases of survivability are attack detection, damage confinement, damage assessment and repair, and attack avoidance focusing on continued service and recovery.
17	The capacity of a system to provide essential services even after successful intrusion and compromise, and to recover full services in a timely manner.
18	Network design and management procedures to minimize the impact of failures on the network.
19	Defined in the terms of a telecommunications network where it is the ability of the network to maintain or restore an acceptable level of performance in the event of deterministic or random network failures, such as link failures and node failures.

20	Defined in terms of performance where it will ensure that, under given failure scenarios, network performance will not degrade below predetermined levels.
21	The ability of a network to cope with facility outages, capacity overloads, and natural disasters.
22	The measure of the degree of keeping the performances of a kind of military weaponry or equipment's or other military forces, which undergoing enemy's attacks.
23	The measure of a network's endurance in the presence of possible component failures (of the measure of the magnitude of attack needed to render a network non-functional).
24	The ability of an item to perform a required function at a given instant in time after a specified subset of components of the item to become unavailable.
25	Where survivable network must achieve an acceptable level of performance under demanding conditions.
26	The assurance of stored information's integrity, confidentiality, and continuous availability guaranteed over time.
27	Defined in terms of survivable information systems through adaptation where it is allowing a system to continue running, albeit with reduced functionality or performance in the face of reduced resources, attacks, or broken components is often preferable to either complete shutdown or continued normal operation in compromised mode.
28	Defined in terms of a survivable system where it must be adaptable, able to respond to attacks and achieve its goals.
29	The capability of a system to complete its mission in a timely manner, even if significant portions are incapacitated by attack or accident.
30	The degree to which a system can withstand an attack or attacks, and is still able to function at a certain level in its new state after the attack.
31	Defined in terms of a survivable system where it satisfies its survivability specification of essential services and adverse environments.
32	The extent to which the software will perform and support critical functions without failures within a specified period when a portion of the system is inoperable.

III. Prey Polulation Survival as Analogy for Survivability In Cloud Computing

There is abundant evidence of the use of nature analogies to study and inspire inventions in other domains, including computing. As suggested by the authors in [8], the use of nature systems for creative and novel solutions to human problems is now common place. For instance, a predator-prey analogy postulating computing infrastructures as homogenously susceptible to attacks, or susceptibility to attack as being heterogeneous [9]. In this instance, security approaches (homogeneous or heterogeneous) are assumed to focus upon traditional computing's physical infrastructures that exist within a static boundary security fence [10]. Analogies aim to capture unique diversification mechanisms in both homogeneous and heterogeneous environments. While the analogy for cloud computing as a metaphor for the internet synonymous to electricity as a utility [11] has been hugely successful, the increased use of analogies in computing demands coherent and systematic approaches for deciding and translating apt functions, behaviours, mechanisms, etc. from one environment to the next. Despite the glaring opportunities analogies present, failure to systematically decide and translate concepts across domains punctuates what the authors in [8] describe as a fundamental sources of problems within this cross-domain approach, due to the disconnect between nature systems and other domains.

In the remainder of this section, we aim to present the survivability of cloud computing infrastructures, systems or services against deliberate attacks analogous to survival of prey species under constant predation. Our approach maps leaf and high-level attributes of both domains (nature and cloud), focusing upon processes and sub-processes at each level.

A. Survival in Nature

Animals in nature share habitats where an abundance of food is vital for their survival. To avoid dying, predators evolve to increase their chances of catching and eating prey, e.g. speed or strength. Similarly, prey will not survive if without evolving and adapting well enough to avoid or evade capture, e.g. speed, smell, camouflage, poison, etc. Thus, predation avoidance and anti-predation mechanisms are the main attributes of prey diversification that define how prey species behave in order to improve its selection, and survivability [12]. Group size from an evolution perspective, is a leaf attributes which affects the stability of predator-prey ecosystems where one species influences another, and different co-evolutionary parameters have an overall effect on survivability of the ecosystem [13]. In this case, the size of a group directly affects investment in anti-predator behaviours, predation pressures such as death rate, and consequently reproductive cycles of species, which are themselves determents of species extinction and survival. As suggested by [14], animals who live in groups are organised to synchronize their activities and move collectively. Figure 1 below illustrates high-level and leaf attributes in nature, whereupon relationships and interactions among animals where one depends on the other for food and survival are complex [15].

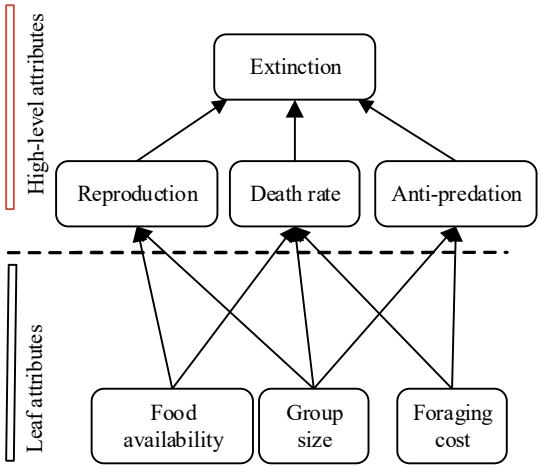

Fig. 1. High-level and leaf attributes for survival in nature

The need to find food necessitates that prey communities are organised to facilitate safety while foraging, primarily against confirmed and potential predators [16]. Similarly, whether prey has an unlimited food source, whether prey suffers very little predation, or whether a prey species is predated by multiple predator species (gazelle hunted by lion, cheetah, wild dogs, hyena) impacts foraging biases and

choices, which in turn impact upon death rates and the evolution of reproduction patterns. Indeed, anti-predator behaviours as a function of prey organisation is therefore attributed to factors such as the abundance of food, predatory behaviours of predators, and the density of predators, among others. In studying mice's anti-predatory behaviors, [17] allude to the notion that prey is indeed aware of the density of predators in their environments and organise themselves accordingly to increase foraging success while avoiding predation.

At a local level, reproduction, predator death rate, migration trends, hunting trends, patterns and intensity of competition, etc. affect the state of a predator-prey ecosystem. The factors exist interactively, whereupon values of one factor depend on the others. As such, the evaluation of the importance of each attribute is determined by the community's overall survival as evidence by population changes and species composition. A common evaluation method is broadly quantified through Lotka and Vito Volterra's equations [18] below: where K is the maximum number of individuals' a given habitat can accommodate and the populations of predators (P) and prey (N) is determined by constant a, b, c, and e, such that:

$$\frac{dN}{dt} = Na(1-\frac{N}{K}) - bNP \qquad (1)$$
$$\frac{dP}{dt} = P(cN - e)$$

A similar approach is used in an experimental simulation to predict the imminent extinction of species in nature. As has been demonstrated and explained in Lotka and Volterra's equations, predator and prey interactions determine the survival or extinction of species. Predation increase the probability of prey extinction and threaten the overall survivability of that specie [5]. In the underlying argument, survivability is thus impacted by an interface of demographic, environmental, and genetic factors and conditions. The ability to avoid and/or counter any threat survival, means that prey communities avoid extinction and improve their overall fitness. Prey offsprings are particularly vulnerable to known predators as they cannot defend themselves, and therefore are highly dependent on their parents.

Population extinction and persistence have applications in ecological studies to describe how species manage to survive over others. In the predator-prey dynamic, predation is considered an environmental stressor on prey survivability [19]. Evidence in ecological studies opinion individualist attributes such as physiological tolerance and fitness in individuals, as expressive of the importance of habitats and competition, and uniquely impact the construction of species communities. Based on the foregoing, we suggest the following as the most important aspects upon which we base our survivability analogy for cloud computing environments:

- The ability to detect triggers such as threats, and institute appropriate countermeasures in a timely manner is reliant upon strategies, technological inventions such as hardware and software, and other techniques.
- Self-management, cooperation, adaptation and the ability to escalate defensive countermeasures enhance survivability.
- Diversity, integration, and the ability for self-management of cloud systems and services enhance survivability.

B. Survivability in Cloud Computing

This section presents our interpretation of the survivability analogy based on prey survival against predation discussed in the section above. The following scenario outlines the pillars for the survivability concept under consideration summarized in Table 2 below.

- Changes in service availability and attacks are oscillatory. An increase in attacks is followed by a decrease in service availability, while a decrease in service availability is followed by a decrease in attacks.
- Where there are very few adversaries, services survivability increases, while very many adversaries cause a decrease in services survivability. However, where there are very many services, adversary survivability increases, however, if there are very few services, adversary survivability decreases.
- Where cooperation is high, the number of thwarted attacks increases and survivability increases, and similarly proactiveness increase services availability.

TABLE 2. PILLARS FOR SURVIVABILITY ANALOGY

Aspect	**Analogy from nature**	**Translation in cloud**
Threats	Prey in groups detects predators, improving survival chances	Ability to detect threats enhances a timeous response, with best strategy or countermeasure
Collective action	Prey's collective foraging biases, predation avoidance methods, and reproduction are a result of evolution and adaptation.	The ability to self-manage, cooperate, adapt and escalate integrated countermeasure techniques means that the number of thwarted attacks increases and survivability increases.
Management	Prey animals' co-habitat to share food, reproduce to improve their fitness and avoid extinction	Diversity, autonomy, integration, and the ability for self-management of cloud systems and services enhance survivability

Fig. 2. below is an illustration of the survivability analogy for cloud computing environments based upon prey survival attributes presented in Fig. 1. Since the business vision of cloud service providers includes assurances for quality, reliability, the availability of services [20], leaf attributes such as recovery time (RT) and recovery objective (RO) as well as sustainable pricing to maximize profits are pertinent to cloud service providers. In this scenario, responsibility for security and availability of services including security affecting the customer's infrastructure lies with the CSP [21]. In a traditional sense, security concerns primarily revolved around the confidentiality, integrity, and availability of information.

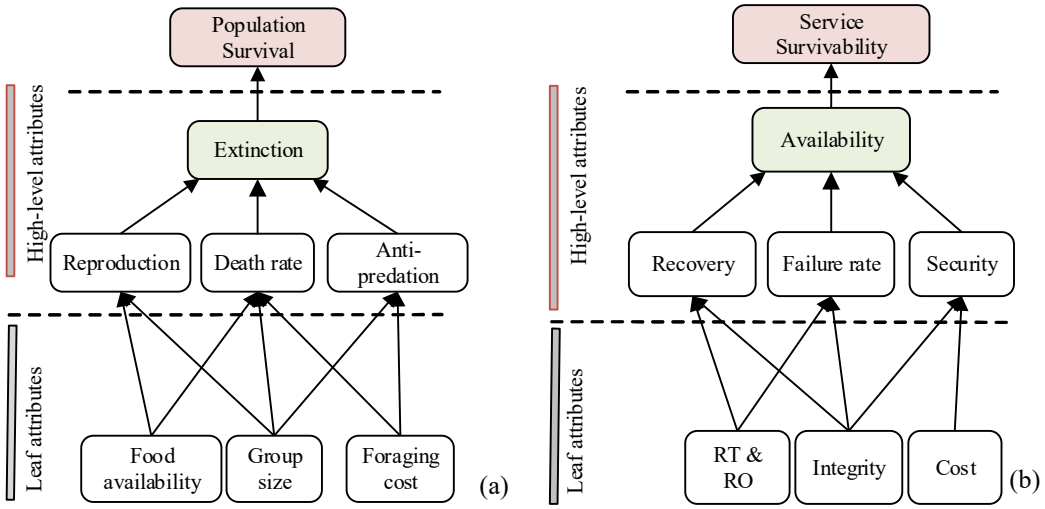

Fig. 2. A visual illustration of prey survivability analogy for cloud computing environments. (a) illustrates the leaf attributes upon which high-level attributes of survival depend. (b) is our translation of this analogy showing leaf attributes upon which the high-level attributes of service survivability depend.

Evidence in literature suggests that predator-prey inspired solutions are successful as perimeter security [22] and worm detection and patching [23]. The analogy being that models with Holling-Ill functional response are useful for describing scenarios where the processing and foraging for food are mutually exclusive and generally prey dependent [24]. Thus, we hypothesise adversary-defender models analogous to predator-prey models as indicative of the defender populations (service availability) in the presence of semantic and flooding DDoS attacks and FRC attacks which are detrimental to a cloud consumer.

While Equation 1 is commonly used to predict the imminent extinction of species in nature and hence their survival, we propose analogous methods for predicting the availability of cloud services and hence their overall survivability. Foremost, cloud services (assuming a cloud service as equivalent to a virtual machine instant) have average probability, ***P***, of being available, where ***VMinUp*** and ***VMnotUp*** represents total number of VMs in a normally and abnormally operating state as described by Equation 2. In addition, the average availability of a virtual machine, ***AV***, is defined as the probability that there are defensive VMs, ***VMax***, (countermeasure agent) available as shown in Equation 3.

$$Av = P(VMinUP \geq VMnotUP) \tag{2}$$

$$AV = P(VMav > 0) \tag{3}$$

$$S_v = (x_t, c_{pd}, r_{vd}) \tag{4}$$

Since virtual machine vulnerabilities to side-channel attacks exposes IaaS to data breaches [25], survivability means that a CSP can guarantee in their SLA, an acceptable level of service despite intentional attack or compromise. Thus, evaluating survivability would consider two main methods: the state of IaaS components (virtual machines), as well as the behaviour of the environment, i.e. whether the infrastructure is operational. Thus, a survivable system should (1) provide availability and security (Integrity and Confidentiality) of services and infrastructures, and (2) meet as closely possible, their expected capacity.

Cause the Operating System (OS) kernel to crash [26] [27] [28] [29]. By logically layering and separating components, CA's lifecycle ensures effective disaster recovery and high availability [30]. BioRAC provide a self-managed platform with high resilience, enabling the availability of services, whether there is a failure, accident or attack [31].

C. Survivability Definition

Survivability in cloud environments is viewed as composite notion; the availability of services, resources or infrastructure (availability), prevention of unauthorised disclosure of data (confidentiality), and prevention of unauthorised deletion and/or modification of data (integrity). We take a unified approach, which emphasises as imperative, a high level of proactiveness to thwart black swan events, as well as high capacity to respond to insecurity in a timely and appropriate manner. Thus, we define survivability as the capacity to timely implement a series of proactive survival responses (akin to prey individuals in nature) in recognition to changes within an environment to ensure a high magnitudes of service availability. We characterise survivability in cloud environments according to the following three-tuple events:

- A series of prey-inspired responses to ensure that cloud platforms remain highly available despite intentional or incidental attacks by known or unknown adversaries.
- Proactive strategies implemented in priority according to the severity of an attack as well as the system's requirements
- Escalation of response as an objective function for optimising survivability, where *X = (x1, x2, x3, x4 ...xn)* is a series of prey-inspired survival properties to ensure that cloud environments remain highly available regardless of attacks. Vector *Y = (y1, y2,*

y3…yn) is a series of proactive preferences for the cloud system, and Z is the objective function for optimising survivability in the cloud.

$$E = (X, Y, Z) \tag{5}$$

Thus, evaluating survivability considers two main methods: the state of IaaS components (virtual machines), as well as the behaviour of the environment, i.e. whether the infrastructure is operational. Thus, a survivable system should;

- Provide availability and security (Integrity and Confidentiality) of services and infrastructures.

IV. CONCLUSIONS & FUTURE WORK

This paper sought to develop a survivability analogy for cloud environments based on the survivability metaphor in predator-prey systems by focus upon unique mechanisms prey species employ to enhance their survivability against predation. The proposed solution is based upon the prey community model, where autonomous individuals' local decisions focus upon enhancing the global survival of the community. Mechanisms of avoiding predation employed by prey species are assumed unique to the predator-prey dynamic and central to the survivability of prey species. Thus, a range of escalating predation avoidance behaviours and anti-predation techniques employed by prey are assumed as determinants of prey survivability.

Similarly, mechanisms for defending the cloud, employed as countermeasures, are assumed as unique to the adversary-defender dynamic and therefore central to the survivability of cloud environments. Building upon gap-filling recommendations for addressing current cloud security challenges presented in Chapter 2, a range of escalating proactive techniques (passive to aggressive) employed as countermeasures, are assumed as determinants of survivability in cloud environments. Unlike the single solution approach characteristic in existing cloud security solutions, the community approach enables rapid reaction based on the ability to make local but synchronised decisions, whereupon escalation enables the proposed system to invoke appropriate proactive security responses based on the nature of threat; ranging from passive to aggressive.

Foremost, it entails a systematic process for developing and mapping analogies for the survivability phenomenon, and the development of bespoke cloud-ecological tools and platforms. Since this solution is inspired by nature, the objective is to develop analogies which best describe the inventive approach central to the proposed system.

To enhance the survivability in cloud infrastructures, foremost, proactive strategies including deceptive, pre-emptive, etc. are implemented to maintain the state of the environment at best, or ensures the system copes with any form of destructive encounter (see sections 4.1 for detailed explanation) between adversaries and defenders. Alternatively, that the system should remain unaltered by the same.

Defenders seek out appropriate strategies to meet the survivability objective under the assumption that cloud infrastructures encounter highly diversified threats, from a broad landscape. Furthermore, resources to counteract the implications of such interactions, including technological, strategic, investment and training, are assumed inadequate. Nonetheless, to attain survivability, the system's robustness is paramount. We put forward the claim that the interplay between insecurity and the capability to be secure, describes the concept of survivability. Along these lines, the survivability concept is described as a metric for evaluating the performance of the system under intentional attack [32]. In other works, it is also defined as a system's ability to timely fulfil its mission during an attack or failure. Due to the complexity and multi-disciplinary nature of the proposed system, its development is modular and iterative. The first stage involved investigating survivability in the inspirational predator-prey systems whereupon theoretical designs are developed. The second stage will build upon the former stage focusing upon survivability in cloud environments involved the development of the analogies in cloud environments.

REFERENCES

[1] G. C. Ainsworth and A. S. Sussman, *The Fungal Population: An Advanced Treatise*. Elsevier, 2013.

[2] V. R. Westmark, "A definition for information system survivability," *37th Annu. Hawaii Int. Conf. Syst. Sci. 2004. Proc.*, vol. 00, no. C, pp. 1–10, 2004.

[3] W. Yurcik and D. Doss, "A Survivability-Over-Security (SOS) Approach to Holistic Cyber-Ecosystem Assurance," no. June, 2002.

[4] W. Liu, "Research on cloud computing security problem and strategy," in *Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on*, 2012, pp. 1216–1219.

[5] T. W. Schoener, D. A. Spiller, and J. B. Losos, "Predators increase the risk of catastrophic extinction of prey populations.," *Nature*, vol. 412, no. 6843, pp. 183–186, 2001.

[6] P. AMERICANUS, "A bioenergetic model for the analysis of feeding and survival potential of winter flounder, Pseudopleuronectes americanus, larvae during the period from hatching to metamorphosis," *Fish. Bull.*, vol. 75, no. 3, 1977.

[7] H. Matsuda, M. Hori, and P. A. Abrams, "Effects of predator-specific defence on biodiversity and community complexity in two-trophic-level communities," *Evol. Ecol.*, vol. 10, no. 1, pp. 13–28, 1996.

[8] D. Burke, "AN ABSTRACT OF THE DISSERTATION OF Title: An Autoethnography of Whiteness," 2007.

[9] S. P. Gorman, R. G. Kulkarni, L. A. Schintler, and R. R. Stough, "A predator prey approach to the network structure of cyberspace," in *Proceedings of the winter international synposium on Information and communication technologies*, 2004, pp. 1–6.

[10] Vmw. Symantec, "white paper : cloud securit y Securing the Cloud for the Enterprise A Joint White Paper from Symantec and VMware Securing the Cloud f for or the Enterprise A Joint White Paper from Symantec and VMware."

[11] E. Brynjolfsson, P. Hofmann, and J. Jordan, "Cloud computing and electricity," *Commun. ACM*, vol. 53, no. 5, p. 32, 2010.

[12] E. D. B. Jr, D. R. F. Jr, and E. D. B. III, "Predator avoidance and antipredator mechanisms: distinct pathways to survival," *Ethol. Ecol. Evol.*, vol. 3, no. 1, pp. 73–77, 1991.

[13] A. Sih, G. Englund, and D. Wooster, "Emergent impacts of multiple predators on prey," *Trends Ecol. Evol.*, vol. 13, no. 9, pp. 350–355, 1998.

[14] C. Sueur and O. Petit, "Organization of group members at departure is driven by social structure in Macaca," *Int. J. Primatol.*, vol. 29, no. 4, pp. 1085–1098, 2008.

[15] M. A. Colomer, A. Margalida, D. Sanuy, and M. J. Perez-Jimenez, "A bio-inspired computing model as a new tool for modeling ecosystems: the avian scavengers as a case study," *Ecol. Modell.*, vol. 222, no. 1, pp. 33–47, 2011.

[16] K. L. Enstam, "Effects of habitat structure on perceived risk of predation and anti-predator behavior of Vervet (Cercopithecus aethiops) and Patas (Erythrocebus patas) monkeys," Springer, 2007, pp. 308–338.

[17] J. L. Orrock and R. J. F. Jr, "An island-wide predator manipulation reveals immediate and long-lasting matching of risk by prey," *Proceedings.Biological Sci. / R. Soc.*, vol. 281, no. 1784, p. 20140391, Apr. 2014.

[18] C. M. N. Pinol and R. S. Banzon, "Stability in a population model without random deaths by the Verhulst factor," *Phys. A Stat. Mech. its Appl.*, vol. 390, no. 7, pp. 1295–1299, 2011.

[19] C. J. Lortie *et al.*, "Rethinking plant community theory," *Oikos*, vol. 107, no. 2, pp. 433–438, 2004.

[20] N. Ziring, "The Future of Cyber Operations and Defense," *Warfare*, vol. 14, pp. 1–7, 2015.

[21] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," *Comput. Electr. Eng.*, vol. 39, no. 1, pp. 47–54, 2013.

[22] S. Sidiroglou and A. D. Keromytis, "Countering network worms through automatic patch generation," 2003.

[23] H. Toyoizumi and A. Kara, "Predators: Good will mobile codes combat against computer viruses," in *Proceedings of the 2002 workshop on New security paradigms*, 2002, pp. 11–17.

[24] P.-P. Liu, "An analysis of a predator&prey model with both diffusion and migration," *Math. Comput. Model.*, vol. 51, no. 9, pp. 1064–1070, 2010.

[25] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in *Proceedings of the 16th ACM conference on Computer and communications security*, 2009, pp. 199–212.

[26] D. Hubbard and M. Sutton, "Top threats to cloud computing v1. 0," *Cloud Secur. Alliance*, 2010.

[27] L. Bello and A. Russo, "Towards a taint mode for cloud computing web applications," in *Proceedings of the 7th Workshop on Programming Languages and Analysis for Security*, 2012, p. 7.

[28] S. Kandula, D. Katabi, M. Jacob, and A. Berger, "Botz-4-sale: Surviving organized DDoS attacks that mimic flash crowds," in *Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2*, 2005, pp. 287–300.

[29] F. Shahzad, "State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions," *Procedia Comput. Sci.*, vol. 37, pp. 357–362, 2014.

[30] E. 'Amiri, "CA Identity Manager: Capabilites and Architecture." 2009.

[31] S. Hariri, M. Eltoweissy, and Y. Al-Nashif, "Biorac: biologically inspired resilient autonomic cloud," in *Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research*, 2011, p. 80.

[32] F. Y.-S. Lin, Y.-S. Wang, and M.-Y. Huang, "Effective proactive and reactive defense strategies against malicious attacks in a virtualized honeynet," *J. Appl. Math.*, vol. 2013, 2013.